

## UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America

v.

Jarret Lea

Defendant(s)

Case No.

18-1395-M

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 5/2/17 - 8/29/18 in the county of Bucks in the  
Eastern District of Pennsylvania, the defendant(s) violated:

Code Section

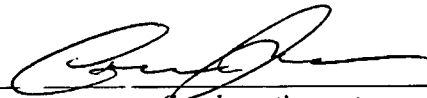
Offense Description

18 U.S.C. § 2252A(g)

Engaging in Child Exploitation Enterprise.

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.


Complainant's signature

Christopher Jackson, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/31/2018


Judge's signature

City and state: Philadelphia, Pennsylvania

Hon. Thomas J. Rueter, U.S. Magistrate Judge

Printed name and title

## **AFFIDAVIT**

I, Christopher Jackson, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed for over two (2) years. I am thus a "federal law enforcement officer," as defined by the Federal Rules of Criminal Procedure. I am currently assigned to the Philadelphia Field Office, in particular to a squad responsible for investigating crimes committed against children, including but not limited to child pornography offenses, in violation of chapter 110 of Title 18, of the United States Code. While employed by the FBI I have investigated federal criminal cases. I have gained experience through numerous hours of training at the FBI Academy, and through everyday work relating to conducting these types of investigations. I have participated in the execution of numerous search warrants for documents and other evidence, including computers and electronic media, in cases involving child pornography and the sexual exploitation of children.

2. This affidavit is being made in support of the issuance of the attached criminal complaint charging Jarret LEA with engaging in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g).

3. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause in support of issuance of the attached complaint, I have not included each and every fact known to me concerning this investigation, but rather only those facts that I respectfully submit are necessary in order to establish probable cause.

### **STATUTORY AUTHORITY**

4. Title 18, United States Code, Section 2252A(g) prohibits any person from engaging in a child exploitation enterprise. In turn, Title 18, United States Code, Section 2252A(g)(2) provides that a person engages in a child exploitation enterprise within the meaning of the section if the person violates (among other portions of Title 18) Chapter 110 of the United States Code, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons. Chapter 110 of the United States Code prohibits, among other offenses, the production of child pornography (18 U.S.C. § 2251(a)); the advertisement of child pornography (18 U.S.C. § 2251(d)); the distribution or receipt of child pornography (18 U.S.C. § 2252(a)(2)); and the possession of child pornography (18 U.S.C. § 2252(a)(4)(B)). Each of the aforementioned violations is a felony offense.

### **PROBABLE CAUSE**

5. On or about May 23, 2017, an FBI online covert employee (OCE) was investigating the production of child pornography on the mobile app “live.me”<sup>1</sup> and browsed to a website called “8ch.net.” On 8ch.net, the OCE observed a link to an URL permitting browser-based access to Service A, a computer-based communication service described further below. Next to the link was an image that depicted two females who appeared to be children wearing bikinis.

6. The OCE clicked on the above link and was re-directed to another URL to a website

---

<sup>1</sup> Live.me is a social media platform for sharing, creating and viewing live streaming videos. Live.me users can stream live video from mobile platforms like Apple iOS or Google Android. Videos streamed from Live.me users can be viewed through the Live.me mobile applications or an internet browser.

operated by Service A-2. This particular website was entitled "Service A-1," and the title was accompanied by a thumbnail image of two minor female children kissing each other.

7. Service A owns and operates a free-access all in one voice and text chat application and website with the same name that can be accessed over the web. A user creates a Service A account and can then communicate with other Service A users.

8. Service A users can exchange private messages between each other, participate in chat discussions, and voice chat. Service A users can also create chat rooms, which functions as message boards that can be accessed only by Service A users who have an invitation link. Service A-1, mentioned above, is one such chat room on Service A. Within these chat rooms, users can set up different sub-rooms wherein users can type written text, including links to files stored on external file-storage sites, and also upload files under a particular size limit, which can be viewed by all users of the sub-room. Service A users can share files larger than the limit allowed by providing hyperlinks to file sharing websites. Service A chat rooms can have one or more moderators. Moderators have the ability to manage other users, including but not limited to removing users from the chat rooms, elevating users hierarchically, and granting users additional permissions. The moderators of a chat room can categorize users of the chat rooms into hierarchical groups with customized labels and can configure those groups to give users in each group different levels of access.

9. The OCE's review of the Service A-1 chat room revealed that the vast majority of its content consisted of discussions about using web cameras and social-media applications to

---

<sup>2</sup> Service A, Service A-1, and similar terms, as well as Username 1 and similar terms, are pseudonyms used in this affidavit in lieu of the actual terms in order to protect the integrity of an ongoing investigation.

obtain sexually-explicit images and videos of minor children; images and videos of minor children exposing their vaginas, which at times were uploaded to the Service A-1 chat room and its sub-rooms; and links to download child pornography images and videos from external file-storage sites. Most of the children viewed by the OCE appeared to be approximately between the ages of 11 and 17 years old. The Service A-1 page also included some discussion of adults engaging in sexual activity via web camera. However, the majority of the activity focused on the depiction of minors engaged in sexually explicit activity on web cameras. For example, in the course of a discussion in the one sub-room of Service A-1 regarding the merits of utilizing virtual private network (VPN) technology to mask users' IP address and identity, Username 1 commented on April 15, 2017: "Just the fact that we're all hanging in here, which is a chatroom where underaged sexual content is shared around is enough reason for one to get a VPN." Username 1 continued, stating: "Fuck when you download something from dropfile Your ISP can see what you downloaded What if govt authorities read ISPs logfiles."

10. Based on the OCE's undercover observations on Service A-1, a federal search warrant was issued, on or about July 10, 2017, by the Honorable David R. Strawbridge, United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Service A's servers related to Service A-1. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of Service A-1, the content of some text chats occurring on Service A-1, and some private messages sent by users of Service A-1.

11. The Service A-1 chat room was ultimately shut down by Service A. Members of the Service A-1 chat room proceeded to open additional similar chat rooms on Service A, including: Service A-2, Service A-3, Service A-4, and Service A-5. The OCE gained access to Service A-3, Service A-4, and Service A-5. The OCE observed each of these chat rooms contained

many of the same users as Service A-1 and were operated for the purpose of discussing, obtaining, and distributing child exploitation material including child pornography files. Service A-5 is the only of the aforementioned Service A chat rooms that is still operating.

12. Based on the OCE's undercover observations on Service A-2, Service A-3, Service A-4, and Service A-5, a second federal search warrant was issued, on or about November 17, 2017, by the Honorable Linda K. Caracappa, Chief United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Service A's servers related to the aforementioned chat rooms. In response to the search warrant, Service A disclosed to law enforcement officers IP address information for some users of those chat rooms, the content of certain text chats occurring in the chat rooms, and some private messages sent by users of those chat rooms.

13. The OCE observed a user of Service A-1 using the online name "Username 11." A review of the search warrant return from Service A and undercover recordings by the OCE revealed, among other activity, the following activity, each involving a video that I have reviewed and that, in my opinion, constitutes a depiction of a minor engaged in sexually explicit conduct as defined by federal law:

a. On May 23, 2017, Username 11 posted on Service A-1:

*"over 2 hr's long. some flashes from 2 girls then 1 girl fingers herself and smells it after at around 44:30 lol then its boring after that http://file.live.ksmobile.net/yolo-[HYPERLINK PARTIALLY REDACTED]--20170523084627.m3u8."*

The OCE utilized the hyperlink to download a video file, which depicted two minor female children who appeared to be under the age of 12. Both of the children exposed their breasts and one of the minor females exposed her vagina and digitally penetrated her vagina.

b. On May 16, 2017, Username 11 posted on Service A-1:

*"http://file.live.ksmobile.net/yolo--[HYPERLINK PARTIALLY REDACTED] --20170501050345.m3u8."* The OCE utilized the hyperlink to download a video file, which depicted a minor female under the age of 12 exposing her vagina.

c. On May 16, 2017, Username 11 posted a link on Service A-1: *"http://file.live.ksmobile.net/yolo- HYPERLINK PARTIALLY REDACTED] --20170515073240.m3u8."* The OCE utilized the hyperlink to download a video file which depicted a minor female under the age of 14 exposing her vagina.

d. On May 2, 2017, Username 11 posted an image on Service A-1. *"http://file.live.ksmobile.net/yolo- HYPERLINK PARTIALLY REDACTED] --20170430072555.m3u8."* The OCE utilized the hyperlink to download a video file which depicted a minor female under the age of 12 exposing her vagina to the camera.

14. Records from Service A show that Username 11 accessed Service A servers using a particular IP address from March 20, 2017 to September 18, 2017. The FBI sent a subpoena to Charter Communications who responded on July 26, 2017. Charter Communications' records showed that the subscriber of the IP address at the relevant times was "Lea Lawanner" at 1900 Interface Lane, Apt. 204, Charlotte, NC 28262.

15. On August 29, 2018, a federal search warrant was executed at 1900 Interface Lane, Apt. 204, Charlotte, NC 28262, LEA's residence. After law enforcement arrived on scene, LEA fled down a third-story balcony and leapt to the ground, suffering injuries requiring hospitalization. LEA's brother, with whom LEA lived at the residence that was the subject of the search, was present during the execution of the warrant. LEA's brother identified and distinguished between digital devices inside the residence that belonged to him, and those that belonged to LEA. LEA's brother explained that he and LEA each owned and used their own digital devices and did not use

or access devices belonging to the other. LEA's brother further explained that the devices were password-protected.

16. From LEA's bedroom, law enforcement officers seized a laptop computer, a desktop computer and three cell phones belonging to LEA. Law enforcement officers conducted an on-scene forensic examination of the devices seized from LEA's bedroom. Preliminary examination of an LG cell phone located on the floor next to LEA's bed revealed that the phone had Service A installed as an application, it had been used to log into Service A as Username 11, and usage of the email account rugerret@gmail.com. Data returned to law enforcement officers by Service A pursuant to a search warrant showed that Username 11 registered for Service A using the e-mail address rugerret@gmail.com. Moreover, on both the laptop and desktop computers located in LEA's bedroom, law enforcement officers located several videos depicting minor children engaged in sexually explicit conduct. In particular, the child pornography videos appeared to be consistent with those distributed by members of the enterprise occurring across Service A-1, Service A-2, Service A-3, Service A-4, and Service A-5, in that the videos appeared to have been created by webcam or similar device, for the apparent purpose of originally being broadcast through an online live video-streaming service.

17. LEA's brother agreed to speak to law enforcement officers. LEA's brother told law enforcement officers that he also used Service A, but only in connection with playing computer games on his desktop computer. Law enforcement officers conducted a preliminary search of LEA's brother's cell phone and did not find the Service A application installed, or any child pornography.



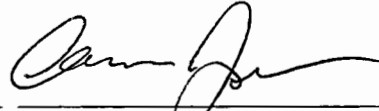
### **VENUE**

18. The child exploitation enterprise in which LEA engaged, as described above, extended at all relevant times to the Eastern District of Pennsylvania. The enterprise was open to members from anywhere in the world, and the child pornography material disseminated by the enterprise was made available to any person able to access Service A, including from the Eastern District of Pennsylvania. Further, the OCE's activities over the various Service A chat rooms comprising the enterprise were conducted in the Eastern District of Pennsylvania. Finally, the investigation has revealed the participation of at least one member of the enterprise who lived in the Eastern District of Pennsylvania and participated in the enterprise from the Eastern District of Pennsylvania, from as early as July 2016 until that member's arrest by federal authorities in February 2018.

### **CONCLUSION**

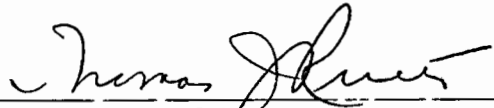
19. Based upon the information above, I respectfully submit that there is probable cause to believe that Jarret LEA engaged in a child exploitation enterprise, in violation of Title 18, United States Code Section 2252A(g), in that LEA violated Chapter 110 of Title 18 of the United States Code as part of a series of felony violations involving three or more separate incidents and more than one victim, and has committed those offenses with three or more other persons. I therefore

further respectfully request that the Court issue the attached complaint and warrant charging LEA with that offense.



\_\_\_\_\_  
Christopher Jackson  
Special Agent, Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED  
BEFORE ME THIS 31 DAY  
OF AUGUST, 2018.



\_\_\_\_\_  
HON. THOMAS J. RUETER  
UNITED STATES MAGISTRATE JUDGE